RNP

Relatório

Geração de Registros de Acesso ao Serviço Eduroam em Base de Dados

Projeto Eduroam-br

Education Roaming em Universidades Brasileiras

Dezembro de 2011

Equipe:

Profa. Débora C. Muchaluat Saade (UFF/IC) - coordenadora
Prof. Célio Vinicius Neves de Albuquerque (UFF/IC)
Prof. Luiz Cláudio Schara Magalhães (UFF/TET)
Prof. Luís Henrique Maciel Kosmalski Costa (UFRJ)
Prof. Miguel Elias Mitre Campista (UFRJ)
Prof. Marcelo Luiz Drumond Lanza (UFRJ)
Prof. Ronaldo Alves Ferreira (UFMS)
Profa. Hana Karina Salles Rubinsztejn (UFMS)
Edelberto Franco Silva (UFF/IC)
Esdras Caleb Oliveira Silva (IC/UFF)
Augusto Tundis Ferreira (UFRJ)
Brivaldo Junior (UFMS)
Juliano T. Bergamo (UFMS)
Péricles C. M. Lopes (UFMS)
Thiago Rodines (UNICAMP)

1. Introdução

O presente relatório apresenta os conceitos envolvidos na implantação da funcionalidade de *accounting* em servidores RADIUS [Radius 00], cujo intuito é armazenar registros referentes às solicitações de acesso realizadas pelos usuários de cada instituição, seja localmente ou em *roaming* entre as universidades envolvidas no projeto. É também introduzido um manual de configuração para a funcionalidade de *accounting* do serviço RADIUS e em complemento à administração desta função, um manual de instalação e configuração do banco de dados PostgreSQL assim como da ferramenta *web, phppgadmin*.

O restante do texto está organizado da seguinte forma. A Seção 2 apresenta os principais conceitos do *accounting*. A Seção 3 exibe um guia de instalação e configuração de todos os serviços envolvidos na realização do *accounting* pelo FreeRADIUS. Na Seção 4, é resumida a busca por ferramentas de visualização e geração de relatórios para os dados de *accounting.* A Seção 5 exibe o status atual do funcionamento do *accounting* nas instituições envolvidas atualmente no projeto. Já a Seção 6 apresenta outras atividades desenvolvidas no período e a Seção 7 conclui o relatório.

2. *Accounting* – Conceitos Básicos

Accounting (também chamado de auditoria) se refere ao monitoramento do comportamento dos usuários e de que forma estes consomem os recursos da rede, e foi introduzido no serviço RADIUS pela RFC 2866 [RFC 2866]. Essas informações podem ser muito úteis, tanto sob a ótica gerencial, quanto, por exemplo, para contabilização e cobrança de serviços (*billing*), além de auxiliar na visão global da demanda da rede, por exemplo, na geração de estatísticas a partir dos dados coletados.

Há muito tempo já se utiliza o *accounting* em provedores de acesso à Internet (ISP – *Internet Service Provider*), surgindo como ferramenta essencial à contabilização da utilização dos serviços para futura cobrança, principalmente, durante a fase de popularização do acesso discado *(dial-up).* Para que sua principal funcionalidade seja desempenhada é interessante que os registros sejam armazenados em um banco de dados. A partir deste armazenamento, é possível extrair informações referentes tanto ao tempo de utilização quanto ao sucesso ou não de uma autenticação solicitada por um usuário, por exemplo.

Conceitos chave necessários ao estudo do *accounting* podem ser listados como:

- **Modelo cliente-servidor:** composto pelo NAS (*Network Access Server*) - que pode ser considerado como o ponto de acesso (AP) à rede, àquele responsável pela comunicação entre o cliente o provedor remoto de recursos (*e.g.* Servidor RADIUS) – que é quem encaminha os dados ao servidor de *accounting* do RADIUS,

que por sua vez retorna com a resposta do cliente, indicando sucesso ou não em sua identificação e liberação de acesso.

- **Segurança de rede:** a comunicação do *accounting* está relacionada à segurança de comunicação do servidor RADIUS, onde, por padrão utiliza-se uma comunicação UDP e senha compartilhada, porém, podendo, no caso da utilização do *accounting* para *roaming,* funcionar sob o RadSec (TCP/TLS).

Cada pacote RADIUS *accounting* é encapsulado em um segmento UDP, cuja porta de destino, por padrão, é a 1813.

Os passos de registro realizados pelo servidor de *accounting,* podem ser descritos como: quando um cliente inicia uma conexão com o servidor RADIUS que dispõe da função de *accounting* habilitada, é gerado e enviado pelo NAS um pacote de requisição de "ínicio" da sessão do cliente, que deverá ser armazenado (provavelmente em um banco de dados). O NAS do cliente recebe também um pacote de retorno sobre a requisição enviada. A Figura 1 mostra as operações mais básicas realizadas pelo *accounting*, o *Accounting-Request* e o *Accounting-Response*, correspondentes, respectivamente ao pedido de armazenamento das requisições do cliente e resposta do servidor RADIUS.

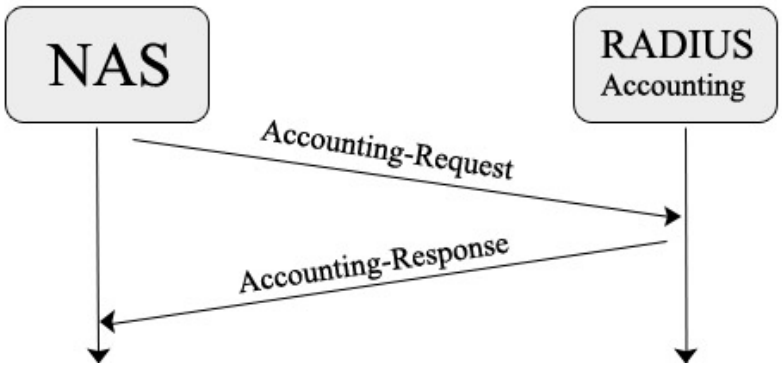

Figura 1 - Registro da requisição de acesso do cliente.

Os atributos de *accounting* carregados no pacote podem conter mais ou menos informações sobre o acesso, dependendo do NAS em questão. Estas informações variam desde o *login* do usuário até o nome e modelo do ponto de acesso contatado. Como complemento, os pacotes de *Accounting-Request* e *Accounting-Response* podem ser referentes ao início (*start*) ou fim (*stop*) de uma sessão, sendo assim é possível contabilizar, por exemplo, o tempo em que o cliente ficou conectado ao serviço.

Após esta breve introdução teórica, serão iniciados os passos de instalação e configuração do *accounting* em um servidor RADIUS.

3. Instalação e configuração do suporte ao *accounting*

Esta seção apresenta um guia passo-a-passo de habilitação do *accounting* para o serviço do FreeRADIUS utilizando como banco de dados o PostgreSQL [PostgreSQL 11]. Primeiramente será apresentada a instalação do banco de dados PostgreSQL. Após esta etapa, será abordado como criar a base de dados utilizada pelo FreeRADIUS para o *accounting*, assim como os arquivos de configuração envolvidos neste processo. Ao final, como complemento e intencionando facilitar a visualização e administração do banco de dados utilizado pelo *accounting* e do PostgreSQL de forma geral*,* é descrita a instalação da ferramenta *phppgadmin.*

3.1. PostgreSQL

A instalação do banco de dados PostgreSQL é simples e necessita apenas de pouca configuração para que esteja em funcionamento. Sendo assim, é necessário realizar apenas os passos das Listagens 1 e 2.

```
# apt-get install postgresql-8.4
```

Listagem 1 - Instalação do PostgreSQL

```
# su - postgres
# psql -c "ALTER USER postgres WITH PASSWORD 'novasenha'"
```

Listagem 2 - Alterando a senha do administrador do PostgreSQL

A Listagem 1 exibe o comando referente à instalação do banco de dados em si, já a Listagem 2 é considerado também um passo importante, uma vez que altera a senha padrão do usuário administrador do banco de dados PostgreSQL.

Caso deseje adicionar algum IP para a administração remota da base de dados, verifique o arquivo contido em *"/etc/postgresql/8.4/main/pg_hba.conf"*. Recomendamos adicionar também o conteúdo da Listagem 3, que representa a liberação do usuário "radius" localmente à base denominada "radius" (que futuramente será criada).

```
local    radius  radius md5
```

Listagem 3 - Liberando usuário "radius" para administração da base de dados

Após a instalação básica do banco de dados é possível passarmos à etapa criação da base de dados utilizada pelo FreeRADIUS para o *accounting*, como será exposto pela Seção 3.2.

3.2. FreeRADIUS

Como primeiro passo, caso o FreeRADIUS tenha sido instalado em uma distribuição com base em pacotes (*e.g.* Ubuntu, Debian), é necessário apenas instalar o pacote com as informações e módulos necessários ao acesso SQL, como na Listagem 4.

```
# apt-get install freeradius-postgresql
```

Listagem 4 - Instalação do suporte ao PostgreSQL pelo FreeRADIUS

Nosso próximo passo, depois de instalado o suporte ao banco de dados, é criar o usuário “radius” que administrará a base de dados chamada “radius”. A base de dados “radius” conterá todas as tabelas necessárias para que o sistema de *accouting* funcione, e seu arquivo SQL é disponibilizado após o passo da Listagem 5.

```
# su - postgres
# createuser radius --no-superuser --no-createdb --no-createrole -P
# createdb radius --owner=radius
# exit
```

Listagem 5 - Criando usuário e base de dados "radius"

Os arquivos relacionados ao *accounting* se encontram na pasta “*/etc/freeradius/sql/postgresql*” e a partir de um dos arquivos lá presentes que serão criadas as tabelas referentes à base de dados “radius criada, como pode ser visto pela Listagem 6.

```
# cd /etc/freeradius/sql/postgresql/
# psql -U radius radius < schema.sql
```

Listagem 6 - Criando as tabelas da base de dados "radius"

Nesse momento, já temos tanto a base de dados como o usuário que a administrará criados e configurados, então, deve-se configurar os arquivos referentes ao FreeRADIUS para habilitar a gravação no banco de dados.

Os arquivos do FreeRADIUS que deverão ser alterados são:

- `/etc/freeradius/sql.conf`
- `/etc/freeradius/sites-enabled/default`
- `/etc/freeradius/radiusd.conf`
- `/etc/freeradius/sql/postgresql/dialup.conf`

No arquivo *“/etc/freeradius/sql.conf”* deverá ser alterada apenas a senha do usuário “radius” e o endereço do servidor de banco de dados, como na Listagem 7.

```
sql {
       database = "postgresql  "
       driver = "rlm_sql_${database}"
```

```
        server = "localhost"
        login = "radius"
        password = "senha_do_usuario_radius_no_bd"
        radius_db = "radius"
                                    .
                                    .
                                    .
}
```

Listagem 7 - Configuração de conexão do RADIUS com a base de dados

É necessário habilitar o *accounting* nos arquivos de configuração do FreeRADIUS, que já estão configurados em sua instalação. Estes arquivos são apresentados pela Listagem 8 e Listagem 9, equivalentes respectivamente aos arquivos "/etc/freeradius/sites-enabled/default" e "/etc/freeradius/radiusd.conf".

```
...
accounting {
        detail
        daily
        unix
        radutmp
        sql
        exec
        attr_filter.accounting_response
  }
...
session {
        radutmp
        sql
}
...
```

Listagem 8 - Ativação do *accounting* no FreeRADIUS

```
...
modules {
        $INCLUDE ${confdir}/modules/
        $INCLUDE eap.conf
        $INCLUDE sql.conf
}
...
```

Listagem 9 - Indicação da configuração de conexão ao SQL

Para que sejam armazenadas as requisições e respostas de forma simultânea para solicitações de autenticação dos usuários, é necessário realizar a configuração do arquivo "*/etc/freeradius/sql/postgresql/dialup.conf*", conforme a Listagem 10.

```
...

simul_count_query   =   "SELECT   COUNT(*)   FROM   ${acct_table1}   WHERE
```

```
  UserName='%{SQL-User-Name}' AND AcctStopTime IS NULL"

simul_verify_query  =  "SELECT  RadAcctId,  AcctSessionId,  UserName,
  NASIPAddress,    NASPortId,    FramedIPAddress,    CallingStationId,
  FramedProtocol FROM ${acct_table1} WHERE UserName='%{SQL-User-Name}'
  AND AcctStopTime IS NULL"

...
```

Listagem 10 - Liberando o armazenamento de conexões simultâneas.

Feitas as configurações, o ideal é que seja reiniciado o serviço do FreeRADIUS em modo *debug* e sejam acompanhadas as tentativas de conexão com o banco de dados.

Para a visualização dos dados armazenados, aconselhamos que sejam seguidos os passos a serem expostos na Seção 3.3, que faz referência à instalação da ferramenta web *phppgadmin*.

3.3. Phppgadmin

Foi instalada uma ferramenta web para administração do banco de dados PostgreSQL, onde é possível visualizar os dados de solicitações de acesso coletados pelo *accounting* do FreeRADIUS.

A instalação desta interface de administração *web* se mostrou simples e pode ser acompanhada a seguir.

Caso não tenha instalado um servidor *web* em seu servidor, aconselhamos a instalação do Apache e, ao menos, o suporte à linguagem PHP em sua última versão, como pode ser visto pela Listagem 11.

```
# apt-get install apache2
# apt-get install libapache2-mod-php5
```

Listagem 11 - Instalação do Apache 2 e suporte a PHP5.

Após a instalação do servidor *web*, e como já temos nosso servidor de banco de dados PostgreSQL instalado e configurado (Seção 3.1), podemos instalar o *phppgadmin*, conforme a Listagem 12.

```
# apt-get install phppgadmin
```

Listagem 12 - Instalação do phppgadmin.

Por padrão, o *phppgadmin* irá aceitar somente conexões vindas da máquina local, portanto, caso deseje acessar a base de dados de outro computador, pela interface *web,* aconselhamos que altere o arquivo localizado em “/etc/phppgadmin/apache.conf” como na Listagem 13. O mesmo arquivo pode já estar contido em “/etc/apache2/conf.d/”, com o nome de *phpgadmin*, e sendo assim, será este que deverá ser alterado. Porém, caso exista apenas o

arquivo “/etc/phppgadmin/apache.conf”, copie-o para a pasta correta, conforme a Listagem 14.

```
Alias /phppgadmin /usr/share/phppgadmin/

<Directory /usr/share/phppgadmin/>

DirectoryIndex index.php

Options +FollowSymLinks

AllowOverride None

order deny,allow

deny from all

allow from seu_ip/mascara

#allow from 127.0.0.0/255.0.0.0 ::1/128

#allow from all

<IfModule mod_php5.c>

  php_flag magic_quotes_gpc Off

  php_flag track_vars On

  php_value include_path .

</IfModule>

</Directory>
```

Listagem 13 - Configuração do arquivo do phppgadmin.

```
# cp /etc/phppgadmin/apache.conf /etc/apache2/conf.d/phppgadmin
```

Listagem 14 - Cópia do arquivo de configuração do Apache para o phppgadmin.

É necessário reiniciar o servidor *web* Apache para que as configrações tenham efeito, este passo é compreendido pela Listagem 15.

```
# /etc/init.d/apache2 restart
```

Listagem 15 - Reiniciando o Apache com as novas configurações.

Para acessar a interface *web* do *phppgadmin* utilize o navegador da máquina em que o acesso foi liberado (Listagem 13) e insira o endereço

"*http://maquina_servidor_postgresql/phppgadmin"*. Será visualizada uma tela como a Figura 2. O acesso aos dados foi realizado pelo usuário "*radius*" que criamos durante a ativação do *accounting,* na Seção 3.2.

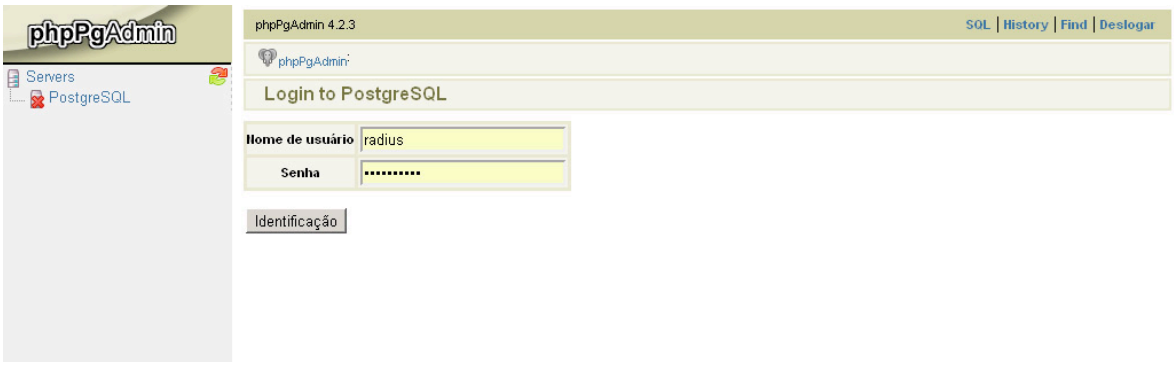

Figura 2 - Tela de acesso do *phppgadmin*.

Uma vez autenticado no sistema, deverá ser selecionada a base de dados que desejamos administrar, no caso, a chamada "*radius*". Como pode ser visto na Figura 3.

Figura 3 - Seleção do banco de dados "radius".

Os dados armazenados na tabela "*radpostauth"* equivalem à resposta da solicitação de autenticação do cliente, e pode ser visualizada pela Figura 4. A partir deste relatório, é simples encontrar se um acesso foi negado ou aceito a um cliente em especial, e em qual momento isto ocorreu.

phpPgAdmin
Servers
PostgreSQL
postgres
radius
Esquemas
public
Tabelas
nas
radacct
radcheck
radgroupch
radgrouprep
radippool
radpostauth
radreply
radusergrou
Visualizações
Sequências
Funções
Domains
Full Text Search
1 2 3 Próximo Last >>
Ações | id | username | pass | reply | calledstationid | callingstationid | authdate
Editar | Deletar | 1 | teste@midiacom.uff.br | teste123 | Access-Accept | NULL | NULL | 2011-12-09 16:14:10.06366-02
Editar | Deletar | 2 | teste@midiacom.uff.br | SenhaErrada=21 | Access-Reject | NULL | NULL | 2011-12-09 16:14:57.236136-02
Editar | Deletar | 3 | teste@midiacom.uff.br | Chap-Password | Access-Accept | NULL | NULL | 2011-12-09 16:16:48.989808-02
Editar | Deletar | 4 | teste@midiacom.uff.br | teste123 | Access-Accept | NULL | NULL | 2011-12-09 16:18:35.696373-02
Editar | Deletar | 5 | teste@midiacom.uff.br | Chap-Password | Access-Accept | NULL | NULL | 2011-12-09 16:18:36.761994-02
Editar | Deletar | 6 | teste@midiacom.uff.br | Chap-Password | Access-Accept | NULL | NULL | 2011-12-09 16:50:16.478408-02
Editar | Deletar | 7 | teste | Chap-Password | Access-Accept | NULL | NULL | 2011-12-12 13:46:27.429422-02
Editar | Deletar | 8 | edelberto | Chap-Password | Access-Reject | NULL | NULL | 2011-12-12 13:53:12.660675-02
Editar | Deletar | 9 | | Chap-Password | Access-Reject | NULL | NULL | 2011-12-12 14:37:13.034032-02
Editar | Deletar | 10 | teste | Chap-Password | Access-Accept | NULL | NULL | 2011-12-12 15:48:42.445194-02
Editar | Deletar | 11 | rafael | Chap-Password | Access-Accept | NULL | NULL | 2011-12-12 17:55:19.458576-02
Editar | Deletar | 12 | caleb | Chap-Password | Access-Accept | NULL | NULL | 2011-12-12 18:29:58.509749-02
Editar | Deletar | 13 | admin | Chap-Password | Access-Reject | NULL | NULL | 2011-12-12 20:27:12.049404-02
Editar | Deletar | 14 | admin | Chap-Password | Access-Reject | NULL | NULL | 2011-12-12 20:27:39.652498-02
Editar | Deletar | 15 | teste | Chap-Password | Access-Accept | NULL | NULL | 2011-12-13 16:10:40.190008-02
Editar | Deletar | 16 | esilva@midiacom.uff.br | Chap-Password | Access-Reject | NULL | NULL | 2011-12-13 16:12:04.104805-02
Editar | Deletar | 17 | esilva@midiacom.uff.br | Chap-Password | Access-Reject | NULL | NULL | 2011-12-13 16:12:08.721341-02
Editar | Deletar | 18 | esilva@midiacom.uff.br | Chap-Password | Access-Reject | NULL | NULL | 2011-12-13 16:13:00.206265-02
Editar | Deletar | 19 | esilva@midiacom.uff.br | Chap-Password | Access-Reject | NULL | NULL | 2011-12-13 16:13:16.940131-02
Editar | Deletar | 20 | esilva@midiacom.uff.br | Chap-Password | Access-Accept | NULL | NULL | 2011-12-13 16:26:27.060373-02
Editar | Deletar | 21 | a | Chap-Password | Access-Reject | NULL | NULL | 2011-12-13 17:31:23.885334-02
Editar | Deletar | 22 | admin | Chap-Password | Access-Reject | NULL | NULL | 2011-12-13 17:31:47.097817-02
Editar | Deletar | 23 | esilva@midiacom.uff.br | Chap-Password | Access-Accept | NULL | NULL | 2011-12-13 18:14:05.649209-02
Editar | Deletar | 24 | esilva@midiacom.uff.br | Chap-Password | Access-Accept | NULL | NULL | 2011-12-13 18:14:18.720233-02
Editar | Deletar | 25 | esilva@midiacom.uff.br | Chap-Password | Access-Reject | NULL | NULL | 2011-12-13 18:17:02.752457-02
Editar | Deletar | 26 | esilva@midiacom.uff.br | Chap-Password | Access-Reject | NULL | NULL | 2011-12-13 18:17:02.811524-02
Editar | Deletar | 27 | esilva@midiacom.uff.br | Chap-Password | Access-Reject | NULL | NULL | 2011-12-13 18:17:08.597145-02
Editar | Deletar | 28 | esilva@midiacom.uff.br | Chap-Password | Access-Accept | NULL | NULL | 2011-12-13 18:17:48.285094-02
Editar | Deletar | 29 | esilva@midiacom.uff.br | Chap-Password | Access-Accept | NULL | NULL | 2011-12-13 18:18:21.537277-02
Editar | Deletar | 30 | caleb | Chap-Password | Access-Reject | NULL | NULL | 2011-12-13 21:14:31.785872-02

Figura 4 - Relatório de requisição de autenticação dos usuários.

Diversos dados podem ser habilitados para a coleta pelo *accounting* e armazenados no banco de dados, aumentando assim as possibilidades de controle e avaliação do ambiente RADIUS administrado.

4. Outras ferramentas de visualização

Foram avaliadas três outras ferramentas de visualização para os dados coletados pelo *accounting*. Foram elas: a ferramenta gratuita recomendada pelos desenvolvedores do FreeRADIUS, freeradius-dialupadmin [Dialup 10], uma ferramenta direcionada à função de *billing,* NETAMS [Netams 07] e também analisada a ferramenta Raptor [Raptor 11]. Esta última ferramenta mostrou que pode ser promissora futuramente, por ter um bom suporte para serviços como o Shibboleth [Shib 11], porém ainda não disponibiliza o suporte ao *accounting* do RADIUS, apesar de comentar que poderá ter suporte estendido a este. As demais ferramentas não se mostraram de simples utilização para o usuário final e, não atenderam a alguns objetivos básicos, como a realização de uma simples busca de autenticações bem sucedidas em certo período do tempo.

Sendo assim, estabeleceu-se a intenção do desenvolvimento de uma ferramenta *web* que, mesmo que simples, auxilie o administrador a obter dados objetivos e rapidamente da base de dados do *accounting.*

5. Status atual da implantação do *Accounting*

Nesta seção são expostos os status de cada uma das instituições participantes, em relação à implantação do *accounting*, até o momento. A Tabela 1 apresenta o panorama atual.

Tabela 1 - Status da implantação do *Accounting*.

Instituição	*Accounting* em funcionamento?
UFF	**SIM**
UFRJ	**em andamento**
UFMS	**SIM**
UFES	**NÃO**
UFRGS	**NÃO**
UNICAMP	**SIM**
UFSC	**NÃO**
UFMG	**NÃO**

6. Outras Atividades

Durante o período foram realizadas outras atividades no âmbito do projeto, como o suporte às instituições interessadas para que se integrem ao projeto eduroam. Além da UFMG, que se encontra em fase de testes de roaming entre instituições, foi dado início à integração da UFPA, que ainda está instalando a infraestrutura RADIUS necessária ao oferecimento do serviço.

Foram feitos testes de roaming internacional com um usuário da University of Waterloo, no Canadá, utilizando o serviço eduroam através da rede da UFRJ. A autenticação foi bem sucedida, mostrando que o piloto eduroam-br está conectado, não só a Europa, mas às outras confederações internacionais também.

A documentação disponível no site do projeto www.midiacom.uff.br/eduroam-br foi ampliada, incluindo uma página de FAQ (*frequently asked questions*) com esclarecimentos gerais sobre o serviço eduroam.

7. Conclusões

Este documento apresentou os conceitos envolvidos na função de *accounting* para o serviço RADIUS a ser incorporado ao projeto eduroam-br como forma de visualização e gerência das solicitações de autenticação recebidas pelos servidores RADIUS das instituições participantes. Foi também

exposto um roteiro de configuração do *accounting* para um servidor FreeRADIUS com todo o embasamento ferramental envolvido neste processo, passando pela habilitação do módulo do FreeRADIUS até a ferramenta *web* de administração do banco de dados PostgreSQL.

A partir deste relatório, acredita-se fornecer uma base tanto do intuito do emprego do *accounting* em um servidor RADIUS, assim como a realização de sua habilitação e configuração. Acredita-se também que o processo de análise e extração de informação dos dados armazenados pelo serviço sejam incrementais, e, portanto, novas ferramentas e visualizadores poderão ser criados durante os próximos passos do projeto.

8. Bibliografia

[Dialup 10] Dialup Admin Administration Interface, 2010, disponível em http://sourceforge.net/projects/dialup-admin/

[Netams 07] Network Traffic Accounting and Monitoring Software, 2007, disponível em http://www.netams.com/netams4_en.html

[PostgreSQL 11] Site oficial, disponível em http://www.postgresql.org

[Radius 00] Remote Authentication Dial In User Service (RADIUS), IETF RFC 2865, junho de 2000.

[Raptor 11] RAPTOR Project, 2011, disponível em http://iam.cf.ac.uk/trac/RAPTOR

[RFC 2866] RADIUS Accounting, 2000, disponível em http://www.ietf.org/rfc/rfc2866.txt

[Shib 11] Shibboleth – A Project of the Internet2 Middleware Initiative, 2011, disponível em http://shibboleth.internet2.edu/